Advisory 2019-005: Remote Code Execution in Remote Desktop Service ("*Dejablue*")

Publication Date	03/09/2019
Last Update	03/09/2019
Current Version	1.0
Relevance	High
Related CVE	CVE-2019-1181, CVE-2019-1182

Summary

A KnowledgeBase article [1] of Microsoft describes a remote code execution vulnerability within the Remote Desktop Service.

Appearance

Beckhoff IPCs with Microsoft Operating Systems like Windows Embedded Standard 7 as well as Windows 7 SP1, Windows Server 2008 R2 SP1 and Windows 10 and related server versions.

Description

On August 13th, 2019 Microsoft published a blog article [1] about remote execution via Remote Desktop Service. This can be misused to run malware on devices that are reachable over the network and have Remote Desktop Service enabled. Operating system updates are available for

- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows 10 and related server versions

Solution

Apply these operating system updates:

Operating System	*Article*	*Download*
Windows 10 Version 1607 for x64-based Systems	KB4512517[1]	Security Update
Windows 10 Version 1607 for x86-based Systems	KB4512517[1]	Security Update
Windows 7 for x64-based Systems	KB4512506	Monthly Rollup
Windows 7 for x86-based Systems	KB4512506	Monthly Rollup
Windows 7 for x64-based Systems	KB4512486	Security Only
Windows 7 for x86-based Systems	KB4512486	Security Only
Windows Embedded Standard 7 for x64-based Systems	KB4512506	Monthly Rollup
Windows Embedded Standard 7 for x86-based Systems	KB4512506	Monthly Rollup

[1] Microsoft strongly recommends you install the latest servicing stack update (KB4509091) for your operating system before installing the latest cumulative update (LCU).

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-securityincident@beckhoff.com
www.beckhoff.com

Windows Embedded Standard 7 for x64-based Systems	KB4512486	Security Only
Windows Embedded Standard 7 for x86-based Systems	KB4512486	Security Only

Beckhoff has evaluated the patches from Microsoft for use with Beckhoff TwinCAT (TwinCAT 3.1 Build 4022.30 and TwinCAT 2 Build 2304) and found no real-time performance impacts. Beckhoff takes this as an indication that applying these patches does not harm the real-time capabilities. However, Beckhoff cannot foresee all changes of the patch on all variations of software in the field. Please note that the patches are cumulative. For older TwinCAT versions, this means that the handling of Advisory 2019-01 [4] must be applied.

Install Microsoft operating system updates

Beckhoff recommends creating a backup before installing updates so that the previous status can be restored at any time. This can be achieved with the Beckhoff Service Tool (BST). More information on the BST can be found on Beckhoff website at https://www.beckhoff.com/english.asp?industrial_pc/bst.htm.

This operating system update for Windows can be retrieved from [2] and [3]. Disclaimer: Beckhoff is not responsible for any side effects negatively affecting the real-time capabilities of your TwinCAT control application possibly caused by updates. Beckhoff offers update images with qualified performance for Beckhoff hardware from time to time. TwinCAT System Manager offers tools, which can be of assistance to verify real-time performance after update. Only administrators or IT experts should perform the backup and update procedure

Mitigation

If the solution is not applicable due to own tests, Beckhoff recommends to

- Disable Remote Desktop Services if not required
- Block Port 3389 in perimeter firewall

Reporting vulnerabilities

Beckhoff Automation welcomes responsibly coordinated reports of vulnerabilities and Beckhoff will collaborate with reporting parties to fix vulnerabilities or mitigate threats.

Additional Resources

[1] Microsoft Publication: https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/

[2] Microsoft Patches for Windows 10 version 1607 and Windows Server 2016:
https://support.microsoft.com/en-us/help/4512517/windows-10-update-kb4512517

[3] Microsoft Patches for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1
https://support.microsoft.com/en-us/help/4512506/windows-7-update-kb4512506

[4] Spectre-V2 and impact on application performance as well as TwinCAT compatibility
https://download.beckhoff.com/download/Document/product-security/Advisories/advisory-2019-001.pdf

History

V 1.0	03/09/2019	Publication

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-securityincident@beckhoff.com
www.beckhoff.com